Access Control Policy Configuration Support System for MAC-Enabled OS

Shunichi Konno Yoichi Hirose
Jumpei Watase Takemi Nisase Mitsutaka Itoh
NTT Information Sharing Platform Laboratories, NTT Corporation
E-Mail: konno.shunichi@lab.ntt.co.jp

Abstract

The Mandatory Access Control (MAC) is being keenly focused as a technology for hardening servers and minimizing the damage of cracking. NSA SELinux is one of the implementations of the MAC mechanism which has merged with the main stream of the Linux kernel and is expected to become widely used. The access control policy is an implementation of the security policy which should reflects a security goal of an organization, and is indispensable to the MAC. However, the SELinux can be only managed by a handful of engineers who has deep knowledge of the software development, the network security and the MAC because the configuration of the access control policy is complicated and is difficult to generate automatically in general. Therefore, by developing a mechanism to make the configuration easier, more people including system administrators will be able to manage the MAC-enabled OS and solve many of the network security issues.

Though the access control policy is written by hand now to reflect a person's will, many parts of the access control policy can be configured systematically. That is, by analyzing the application source code and its configuration file, the basic structure of the access control policy can be generated. With some additional information such as naming rules of the access control policy, system standard file hierarchy and hardware component of the target system including network interfaces, system dependent parameters and values are finally determined. For example, by checking file access functions in the application source code, we can generate file access "allow" rules as the access control policy. Based on this idea, we implemented a part of the "Access Control Policy Configuration Support System." Using this system, the access control policy to run an application under MAC will be configured much easier. In this system, the person's will can also be reflected interactively during the access control policy configuration process.

In this presentation, we would like to show which part of the access control policy can be configured systematically, and propose the system to generate the access control policy from the application source code. We also discuss the environment in which the information to configure the access control policy can be properly extracted from the application source code, the application configuration file and other additional inputs.